

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-185376

(43)Date of publication of application : 16.07.1996

(51)Int.Cl.

G06F 15/00

H04L 9/00

H04L 9/10

H04L 9/12

(21)Application number : 06-327267

(71)Applicant : HITACHI LTD

(22)Date of filing : 28.12.1994

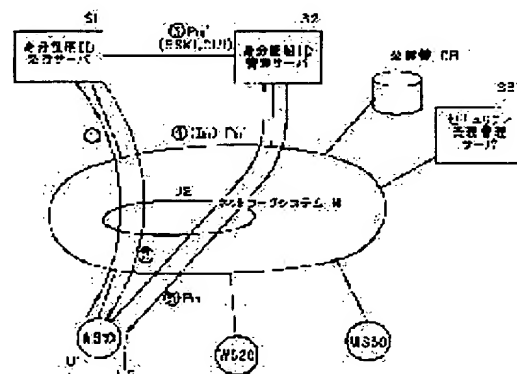
(72)Inventor : SAITO YOKO

(54) MESSAGE TRUST SYSTEM

(57)Abstract:

PURPOSE: To improve the reliability of security work for a highly secret message transmitted/received through a network.

CONSTITUTION: An identification(ID) issuing server S1 and an ID managing server S, issue an ID card IDPU inherent in a user U1 in accordance with the request from the user U1. The user U1 presents a trust condition for a message to a security work managing server S3 by the use of the ID card IDPU1 and the server S3 executes security work such as the storage, publication and cancelation of the message based upon the trust condition. Data communication through a network N protects the secrecy of the ID card IDPU1 and the message by an open key ciphering system. In addition, evidence information indicating that a preparator is the user U1 himself (or herself) and evidence information proving that the ID card IDPU1 is an original are added to a trusted message.



LEGAL STATUS

[Date of request for examination]

10.02.1998

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平8-185376

(43) 公開日 平成8年(1996)7月16日

(51) Int. Cl.⁵

G 0 6 F 15/00

H 0 4 L 9/00

9/10

9/12

識別記号

3 3 0 A 9364-5L

庁内整理番号

F I

技術表示箇所

H 0 4 L 9/ 00

Z

審査請求 未請求 請求項の数3 O L (全 17 頁)

(21) 出願番号

特願平6-327267

(22) 出願日

平成6年(1994)12月28日

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 齋藤 洋子

神奈川県横浜市戸塚区戸塚町5030番地 株

式会社日立製作所ソフトウェア開発本部内

(74) 代理人 弁理士 武 順次郎

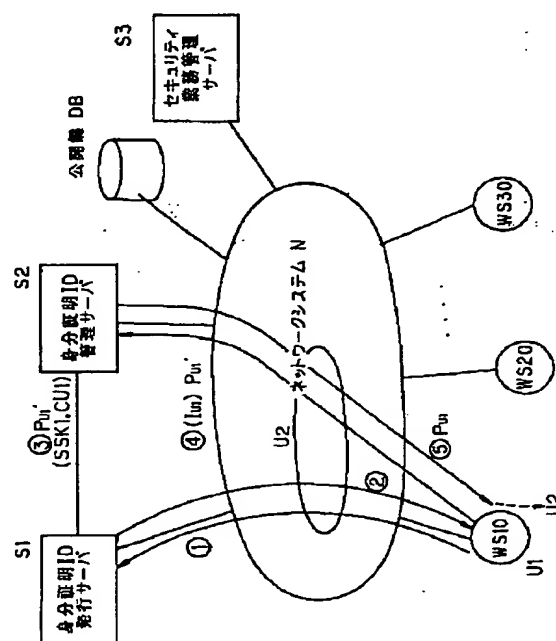
(54) 【発明の名称】 メッセージの信託システム

(57) 【要約】 (修正有)

【目的】 メッセージの信託システムに関し、ネットワーク経由で送受信される機密度の高いメッセージについてのセキュリティ業務の信頼性を向上させる。

【構成】 身分証明ID発行サーバ S_1 および身分証明ID管理サーバ S_2 は、ユーザ U_1 からの要求に応じて当該ユーザ U_1 固有の身分証明ID P_{U1} を発行および交付する。ユーザ U_1 は、身分証明ID P_{U1} を用いてセキュリティ業務管理サーバ S_3 にメッセージについての信託条件を提示し、これに基づいてセキュリティ業務管理サーバ S_3 は、メッセージの保管、公開、破棄などのセキュリティ業務を行う。ネットワーク N を介したデータ通信では、公開鍵暗号方式によって身分証明ID P_{U1} やメッセージの機密保護を図る。また、信託するメッセージには、作成者がユーザ U_1 であることを示す証拠情報や、原本であることを証明する証拠情報を付加する。

【図4】



【特許請求の範囲】

【請求項 1】 ネットワークを介して相互に接続された複数のワークステーション間でメッセージの送受信を行うシステムにおいて、

特別なセキュリティ業務を利用するユーザの各々について当該ユーザに固有の身分証明 ID の発行および管理を行う身分証明 ID 登録手段と、

前記セキュリティ業務を利用するために前記身分証明 ID を用いてネットワーク経由で送受信されるメッセージを第三者から秘匿する信託メッセージ秘匿手段と、

前記身分証明 ID を用いてユーザから送信されたメッセージについて当該ユーザが指定した信託条件の通りに前記セキュリティ業務を実行するセキュリティ業務管理手段と、を具備する構成としたことを特徴とするメッセージの信託システム。

【請求項 2】 各々のメッセージについて当該メッセージの生成および送受信があったことを示す証拠情報を作成する証拠情報作成手段と、

前記メッセージのデータ形式を第三者によって改竄不能なデータ形式に変換する改竄防止手段と、をさらに具備する構成としたことを特徴とする請求項 1 記載のメッセージの信託システム。

【請求項 3】 システム内で発生した事象についての履歴情報を取得する履歴情報取得手段と、

前記履歴情報に基づいて前記セキュリティ業務の侵害に関する監査を行うセキュリティ侵害監査手段と、をさらに具備する構成としたことを特徴とする請求項 2 記載のメッセージの信託システム。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明はメッセージの信託システムに係り、特に、ネットワーク経由で機密度の高いメッセージの送受信が行われるメッセージの信託システムに関する。

【0002】

【従来の技術】 従来より、ネットワークを介して接続されているワークステーション（以後、“WS”と略記する）相互間で行われるメッセージの送受信を保証するための技術として、通信回線上の伝送データやファイル中の記録データを暗号化する技術が知られている。また、特開平 5-268595 号公報記載の発明においては、メッセージの内容そのものを保証する方法が提案されており、さらに、特開平 2-189636 号公報記載の発明においては、データ送信元のシステム内にネットワーク内のすべての転送経路を示す経路情報と転送データへのアクセスが許されるシステム群を示すデータ属性とを用いることで送信者が任意の転送経路を選択可能とする方法が提案されている。このほか、メッセージを保管する機能については、一般的に電子メールのメールボックス機能やデータベース機能などによって実現されてい

る。

【0003】

【発明が解決しようとする課題】 上述したメッセージの送受信に関連する従来技術は、メッセージの保証や転送および保管などの個々の機能に対しては有効であるが、業務内容によっては必ずしも有効に適用できない場合がある。例えば、世間一般に認められた機関（法律事務所など）に対して依頼者が何らかのメッセージ（遺言書など）を登録し、一定の条件のもとで対象者に当該メッセージを開示させる（依頼者が死亡した時点で利害関係人に当該遺言書を公開させるなど）という高度なセキュリティを要するサービス業務をペーパーレスで実現しようとする場合、上記従来技術に加えてさらに以下に示すような要件が必要になってしまうという問題点があった。

【0004】 ①信託されたメッセージが“文書”として認められること。

・信託すべきメッセージは所定の形式にしたがって作成されており、特に必要な場合にはシステム管理者や関連機関の承認を経ているなければならない。

【0005】 ・信託すべきメッセージについて、依頼者本人による原本であって、いかなる改竄もなされていないことが保証されなければならない。

【0006】 ②信託されたメッセージが確実に保管管理されること。

・依頼者に登録されたメッセージは、依頼者から指定された信託条件の通りに管理されていないなければならない。

・信託されたメッセージの内容は、第三者に盗用されないように確実に秘匿されなければならない。

・信託されたメッセージに対する第三者の不正なアクセスを防止するため、ネットワークを含むシステム内で発生する動作事象を常に監視しなければならない。

【0007】 したがって本発明の目的は、上記の問題点を解決して、ネットワーク経由で送受信される機密度の高いメッセージについてのセキュリティ業務の信頼性を向上させることのできるメッセージの信託システムを提供することにある。

【0008】

【課題を解決するための手段】

(1) 上記の目的を達成するため、本発明のメッセージの信託システムは、ネットワークを介して相互に接続された複数のワークステーション間でメッセージの送受信を行うシステムにおいて、特別なセキュリティ業務を利用するユーザの各々について当該ユーザに固有の身分証明 ID の発行および管理を行う身分証明 ID 登録手段と、前記セキュリティ業務を利用するために前記身分証明 ID を用いてネットワーク経由で送受信されるメッセージを第三者から秘匿する信託メッセージ秘匿手段と、前記身分証明 ID を用いてユーザから送信されたメッセージについて当該ユーザが指定した信託条件の通りに前記セキュリティ業務を実行するセキュリティ業務管理手段

と、を具備する構成としたものである。

〔0009〕(2) また、(1)において、各々のメッセージについて当該メッセージの生成および送受信があったことを示す証拠情報を作成する証拠情報作成手段と、前記メッセージのデータ形式を第三者によって改竄不能なデータ形式に変換する改竄防止手段と、をさらに具備する構成としたものである。

〔0010〕(3) さらに、(2)において、システム内で発生した事象についての履歴情報を取得する履歴情報取得手段と、前記履歴情報に基づいて前記セキュリティ業務の侵害に関する監査を行うセキュリティ侵害監査手段と、をさらに具備する構成としたものである。

〔0011〕

【作用】上記構成に基づく作用を説明する。

〔0012〕(1) 本発明のメッセージの信託システムは、ネットワークを介して相互に接続された複数のワークステーション(WS)間でメッセージの送受信を行うシステムにおいて、特別なセキュリティ業務を利用するユーザの各々について当該ユーザに固有の身分証明IDの発行および管理を行う身分証明ID登録手段と、前記セキュリティ業務を利用するために前記身分証明IDを用いてネットワーク経由で送受信されるメッセージを第三者から秘匿する信託メッセージ秘匿手段と、前記身分証明IDを用いてユーザから送信されたメッセージについて当該ユーザが指定した信託条件の通りに前記セキュリティ業務を実行するセキュリティ業務管理手段と、を具備している。すなわち、身分証明ID登録手段は身分証明IDによって特別なセキュリティ業務を利用するユーザの身元を保証し、セキュリティ業務管理手段は身分証明IDによる身元の保証が完了しているユーザに対してのみメッセージの信託サービスなどのセキュリティ業務を提供するので、不正に情報を取得しようとする意図を持つ悪質なユーザを容易に選別および排除することができる。そして、信託メッセージ秘匿手段はネットワーク経由で送受信されるメッセージの内容を暗号化して、当該メッセージに関わるユーザおよびセキュリティ業務管理手段以外の第三者に知られないようにするので、仮に悪質なユーザにメッセージを取得された場合でも、その盗用などによる損失の発生を未然に防止することができる。

〔0013〕(2) また、(1)において、各々のメッセージについて当該メッセージの生成および送受信があったことを示す証拠情報を作成する証拠情報作成手段と、前記メッセージのデータ形式を第三者によって改竄不能なデータ形式に変換する改竄防止手段と、をさらに具備している。すなわち、証拠情報作成手段は身分証明IDによってセキュリティ業務を利用するユーザのWSから送信されてきたメッセージについて生成および送受信が行われた事実を証明するための証拠情報を作成するので、セ

場合、保管しておいた証拠情報を調べることによって紛争の原因を客観的に突き止めることができる。そして、改竄防止手段はメッセージの当事者(例えば、メッセージを作成および送信したユーザと、当該ユーザに対してセキュリティ業務を提供するセキュリティ業務管理手段)以外の第三者に改竄されないようにメッセージのデータ形式を変換するので、メッセージの内容についての信頼性を向上させることができる。

〔0014〕(3) さらに、(2)において、システム内で発生した事象についての履歴情報を取得する履歴情報取得手段と、前記履歴情報に基づいて前記セキュリティ業務の侵害に関する監査を行うセキュリティ侵害監査手段と、をさらに具備している。すなわち、履歴情報取得手段は稼働中のシステム内で発生した事象を履歴情報として絶えず記録しており、セキュリティ侵害監査手段は記録された履歴情報を常に分析しているので、悪質なユーザによるセキュリティ侵害を迅速に検出して、早期に適切な処置をとることができる。

〔0015〕

【実施例】以下、本発明のメッセージの信託システムの一実施例を図面を用いて詳細に説明する。

〔0016〕図1は、本発明のメッセージの信託システムの一構成例を示すブロック図である。同図中、ネットワークシステムN上には身分証明ID発行サーバ S_1 、身分証明ID管理サーバ S_2 (S_1 および S_2 が請求項中の“身分証明ID登録手段”に相当する)、セキュリティ業務管理サーバ S_3 (請求項中の“セキュリティ業務管理手段”に相当する)が存在しており、ネットワークを介して接続されたワークステーション WS_{10} 、 WS_{20} 、 WS_{30} から特別なセキュリティ業務の利用要求を行う。以後、セキュリティ業務の一例として、 WS_{10} からネットワークシステムNにアクセスするユーザ U_1 がセキュリティ業務管理サーバ S_3 によるメッセージの信託サービスを利用する場合について説明を行う。なお、他のセキュリティ業務としては、メッセージの保管サービス、伝達サービスなども考えられる。

〔0017〕メッセージの信託サービスを利用する場合、ユーザは身分証明ID発行サーバ S_1 に対して、当該サービスを利用するための特別な身分証明IDの発行を事前に要求し、交付された身分証明IDを用いてメッセージの信託を行う。図2は、身分証明IDの発行要求に伴って図1のシステムで行われるデータ通信について概略的に示す図である。同図中、処理①はユーザ U_1 が身分証明IDである PU_1 の発行を要求する処理であり、処理②は処理①に応じて身分証明ID発行サーバ S_1 からユーザ U_1 に対して仮の引替え証 PU_1' (後日、発行された正式な身分証明IDの交付を受けるための情報)を発行する処理である。処理①において、ユーザ U_1 は自己を特定する識別情報 I_{U1} (通常のユーザIDやパスワードなど)を指定して身分証明ID発行サーバ S_1 に PU_1 の発行

要求を行う。身分証明ID発行サーバ S_1 はこの発行要求を確認した後、処理②でユーザ U_1 に対する仮の引替え証 PU_1' の発行処理を行う。仮の引替え証 PU_1' は正式な身分証明IDの交付を受ける際に必須の情報なので、ユーザ U_1 はこれを大切に保管管理する。また、識別情報 I_{U_1} の内容についても他人に知られないように管理しておく。

【0018】ところで、セキュリティ業務に関わるシステムとして考慮すべき点は、処理①および②に伴って行われるデータ通信の内容について、セキュリティ業務を侵害して不正に情報を取得しようとする意図を持つ悪質なユーザに知られないようにすることであり、このためにはデータ通信される内容を必ず暗号化しておくことが有効である。例えば、ネットワークシステムN内に公知の公開鍵暗号方式（請求項中の“信託メッセージ秘匿手段”および“改竄防止手段”に相当する）を採用し、すべてのユーザ U_i 、身分証明ID発行サーバ S_1 、身分証明ID管理サーバ S_2 、セキュリティ業務管理サーバ S_3 の各々に対して公開鍵および秘密鍵を割当てる。そして、すべてのユーザ U_i の公開鍵 PK_{U_i} 、身分証明ID発行サーバ S_1 の公開鍵 PK_{S_1} 、身分証明ID管理サーバ S_2 の公開鍵 PK_{S_2} 、セキュリティ業務管理サーバ S_3 の公開鍵 PK_{S_3} については、公開鍵データベースを用いて公開し、秘密鍵 SK_{U_i} については各々のユーザ U_i が別のユーザに知られないように保管管理しておく。そして、データ通信の際に自己の秘密鍵と相手の公開鍵を用いて通信内容を暗号化することにより、悪質なユーザを容易に選別および排除するとともに、仮に悪質なユーザに情報を取得されてもその盗用などによる損失の発生を未然に防止することができる。

【0019】図3は、図2のデータ通信における機密保護のための処理の流れを示すフローチャートであり、ユーザ U_1 が自己の秘密鍵 SK_{U_1} と身分証明ID発行サーバ S_1 の公開鍵 PK_{S_1} を用いて処理①に伴うデータ通信を暗号化する場合の一例を示す。図3において、ユーザ U_1 は身分証明ID発行サーバ S_1 に伝えるべき情報 I_{U_1} を秘密鍵 SK_{U_1} で暗号化した後、さらに公開鍵 PK_{S_1} で暗号化して、暗号化メッセージ M ($M=ENC_{PK_{S_1}}(ENC_{SK_{U_1}}(I_{U_1}))$)を作成する（ステップ301）。そして、この暗号化メッセージ M をネットワークNを介して身分証明ID発行サーバ S_1 に送信する（ステップ302）。身分証明ID発行サーバ S_1 は、ネットワークNを介して受信した暗号化メッセージ M を自己の秘密鍵 SK_{S_1} で解読した後、さらにユーザ U_1 の公開鍵 PK_{U_1} で解読して、元の情報 I_{U_1} ($I_{U_1}=DEC_{PK_{U_1}}(DEC_{SK_{S_1}}(M))$)を得る（ステップ303）。ここで、 $ENC_{SK_{U_1}}(I_{U_1})$ の内容を復元することができるのは秘密鍵 SK_{S_1} を管理している身分証明ID発行サーバ S_1 のみであり、さらに公開鍵 PK_{U_1} で復号化して得た元の情報 I_{U_1} の内容を調べることによって処理①（ステップ302）で送信されてきた

メッセージがユーザ U_1 からのものであることを確認できる（ステップ304）。

【0020】同様に処理②についても、身分証明ID発行サーバ S_1 はユーザ U_1 に伝えるべき情報 PU_1' 、 SSK_1 、 CU_1 を自己の秘密鍵 SK_{S_1} で暗号化した後、さらにユーザ U_1 の公開鍵 PK_{U_1} で暗号化して、暗号化メッセージ M ($M=ENC_{PK_{U_1}}(ENC_{SK_{S_1}}(PU_1', SSK_1, CU_1))$)を作成する（ステップ305）。そして、ネットワークNを介してこの暗号化メッセージ M をユーザ U_1 に送信する（ステップ306）。ユーザ U_1 は、ネットワークNを介して受信した暗号化メッセージ M を自己の秘密鍵 SK_{U_1} で解読した後、さらに身分証明ID発行サーバ S_1 の公開鍵 PK_{S_1} で解読して、元の情報 PU_1' 、 SSK_1 、 CU_1 を得る（ステップ307）。ここで、 $ENC_{SK_{S_1}}(PU_1', SSK_1, CU_1)$ の内容を復元することができるのは秘密鍵 SK_{U_1} を管理しているユーザ U_1 のみであり、さらに公開鍵 PK_{S_1} で復号化して得た元の情報 PU_1' 、 SSK_1 、 CU_1 の内容を調べることによって処理②（ステップ306）で送信されてきたメッセージが身分証明ID発行サーバ S_1 からのものであることを確認した後、これらの情報を保管する（ステップ308）。

【0021】なお、処理②において、以降の通信で用いるセッション鍵 SSK_1 や、身分証明ID管理サーバ S_2 に対して身分証明ID PU_1 の取得要求を行う際のアクセス条件 CU_1 を付加しておくことにより、身分証明IDの発行業務をより確実に行うことができる。例えば、アクセス条件 CU_1 によって、指定された期間内に指定されたアクセス経路で身分証明ID管理サーバ S_2 に取得要求を行わせるようにすれば、悪質なユーザの介入をより確実に排除しやすくなる。また、処理①および②でやり取りされる情報の内容、情報の保護のレベル、ユーザの資格審査の具体的な方法などについては、セキュリティ業務の管理に必要とされる機密度に応じて任意に決定される。

【0022】ところで、身分証明ID発行サーバ S_1 はユーザから身分証明IDの発行要求を受付けるが、実際に身分証明IDを準備してユーザへの交付を行うのは身分証明ID管理サーバ S_2 である。これは、身分証明IDの受付から発行までにある程度の時間がかかることが予想されることから、身分証明ID発行サーバ S_1 への発行要求が集中した場合のトラフィック量を考慮したことによる。また、ユーザ U_1 が身分証明ID管理サーバ S_2 に仮の引替え証 PU_1' を提示して身分証明IDの交付を要求することで、ユーザ U_1 の身元を2度にわたって確認できる。すなわち、身分証明ID管理サーバ S_2 は、仮の引替え証 PU_1' を提示して身分証明IDの交付を要求してきたユーザと先に身分証明ID発行サーバ S_1 に対して身分証明IDの発行要求を行ったユーザ U_1 とが同一のユーザであるか否かを確認するとともに、当該ユーザがアクセス条件 CU_1 にしたがって身分証明IDの交付を要求してきたか否かを確認し、いずれかを満たさないユーザから

の身分証明IDの交付要求については拒否するようにする。

【0023】図4は、身分証明IDの登録および発行処理に伴って図1のシステムで行われるデータ通信について概略的に示す図である。同図中、処理③は身分証明ID発行サーバ S_1 が身分証明ID管理サーバ S_2 に対してユーザ U_1 の身分証明ID発行要求を登録する処理、処理④はユーザ U_1 が身分証明ID管理サーバ S_2 に対して身分証明IDの交付を要求する処理、処理⑤は身分証明ID管理サーバ S_2 がユーザ U_1 に対して身分証明ID PU_1 を交付する処理である。ここで、処理③においては、図2を用いて説明した処理②で身分証明ID発行サーバ S_1 がユーザ U_1 に対して発行した仮の引替え証 PU_1' の情報を身分証明ID管理サーバ S_2 に引き渡す。セッション鍵 SSK_1 やアクセス条件 CU_1 が指定されていれば、これらも身分証明ID管理サーバ S_2 に引き渡す。なお、身分証明ID発行サーバ S_1 と身分証明ID管理サーバ S_2 の間では取扱に機密性を要する情報の交換が行われるので、この両者を繋ぐ通信路については十分に保護しておく。例えば、特殊な保護チャネルを使用する、 S_1 および S_2 に対するアクセス管理を厳格に行う、 S_1 および S_2 専用の暗号鍵で暗号化してデータ通信を行う、などによって通信路の保護を図る。

【0024】処理④において、ユーザ U_1 は身分証明ID管理サーバ S_2 に対して自己の識別情報 I_{U1} （処理①で提示した通常のユーザIDやパスワードなど）と仮の引替え証 PU_1' の情報を提示する。処理⑤において、身分証明ID管理サーバ S_2 はユーザ U_1 から提示された情報を確認し、問題がなければ身分証明ID PU_1 を交付する。ここで問題となるのは、身分証明ID PU_1 が悪質な第三者の手に渡ってしまった場合である（例えば、正規のユーザ U_1 に対して交付された身分証明ID PU_1 の内容を悪質なユーザ U_2 が盗み見るといったケースなど）。一般的にユーザ U_1 には自己の身分証明ID PU_1 をきちんと管理する義務があるので、ユーザ U_1 が日常的に使用している WS_{10} から身分証明ID PU_1 が盗まれてしまったときにはユーザ U_1 側に責任がある。しかしながら、ネットワークNにおけるデータ通信の過程で身分証明ID PU_1 が盗まれてしまったときにはセキュリティ業務を提供する側の責任となるので、ユーザ U_1 と身分証明ID管理サーバ S_2 との間のデータ通信の保護を図ることが必要不可欠である。

【0025】図5は、図4のデータ通信における機密保護のための処理の流れを示すフローチャートである。同図中、ユーザ U_1 は身分証明ID管理サーバ S_2 に伝えるべき情報（識別情報 I_{U1} および仮の引替え証 PU_1' など）を秘密鍵 SK_{U1} で暗号化した後、さらに公開鍵 PK_{S2} で暗号化して、暗号化メッセージ M （ $M = \text{ENC}_{PK_{S2}}(\text{ENC}_{SK_{U1}}(I_{U1}, PU_1'))$ ）を作成する（ステップ501）。そして、この暗号化メッセージ M をネットワークNを介して身分証明ID管理サーバ S_2 に送信する（ステップ5

02）。なお、セッション鍵 SSK_1 が指定されている場合、暗号化メッセージ M をさらにセッション鍵 SSK_1 で暗号化してから送信すれば、ステップ502におけるユーザ U_1 と身分証明ID管理サーバ S_2 との間のデータ通信の機密性向上を図ることができる。身分証明ID管理サーバ S_2 は、ネットワークNを介して受信した暗号化メッセージ M を自己の秘密鍵 SK_{S2} で解読した後、さらにユーザ U_1 の公開鍵 PK_{U1} で解読して、元の情報 I （ $I = \text{DEC}_{PK_{U1}}(\text{DEC}_{SK_{S2}}(M))$ ）を得る（ステップ503）。ここで、暗号化メッセージ M から元の情報を復元できるのは秘密鍵 SK_{S2} を管理している身分証明ID管理サーバ S_2 のみであり、さらに公開鍵 PK_{U1} で復号化して得た元の情報 I の内容を調べることによって処理④（ステップ502）で送信されてきたメッセージがユーザ U_1 からのものであることを確認できる。続いて、ユーザ U_1 からのアクセスが指定されたアクセス条件 CU_1 を満たしているかどうかを判定し、満たしていない場合には処理④を拒否する（ステップ504）。

【0026】ユーザ U_1 からのアクセスがアクセス条件 CU_1 を満たしている場合、身分証明ID管理サーバ S_2 はユーザ U_1 に回答すべき情報（身分証明ID PU_1 、以降のデータ通信で用いる新たなセッション鍵 SSK_1 など）を自己の秘密鍵 SK_{S2} で暗号化した後、さらにユーザ U_1 の公開鍵 PK_{U1} で暗号化して、暗号化メッセージ M （ $M = \text{ENC}_{PK_{U1}}(\text{ENC}_{SK_{S2}}(PU_1, SSK_1))$ ）を作成し、ネットワークNを介してこの暗号化メッセージ M をユーザ U_1 に送信する（ステップ505）。なお、セッション鍵 SSK_1 が指定されている場合、暗号化メッセージ M をさらにセッション鍵 SSK_1 で暗号化してから送信すれば、ステップ505における身分証明ID管理サーバ S_2 とユーザ U_1 との間のデータ通信の機密性向上を図ることができる。ユーザ U_1 は、ネットワークNを介して受信した暗号化メッセージ M を自己の秘密鍵 SK_{U1} で解読した後、さらに身分証明ID管理サーバ S_2 の公開鍵 PK_{S2} で解読して、元の情報 PU_1 、 SSK_1 を得る（ステップ506）。ここで、暗号化メッセージ M から元の情報を復元することができるのは秘密鍵 SK_{U1} を管理しているユーザ U_1 のみであり、さらに公開鍵 PK_{S2} で復号化して得た元の情報の内容の調べることによって処理⑤（ステップ505）で送信されてきたメッセージが身分証明ID管理サーバ S_2 からのものであることを確認した後、これらの情報を保管する（ステップ507）。

【0027】一旦、固有の身分証明ID PU_1 が発行されると、ユーザ U_1 はこの身分証明ID PU_1 を用いてセキュリティ業務管理サーバ S_3 にメッセージの信託を依頼することができる。図6は、メッセージの信託処理に伴って図1のシステムで行われるデータ通信について概略的に示す図である。同図中、ユーザ U_1 はどのようなメッセージをどのように信託するかを表す信託条件 CU_2 を、身分証明ID PU_1 を用いてセキュリティ業務管理サーバ S_3 に

10

20

30

40

50

伝える(処理⑦)。そして、信託条件 CU_2 について合意が得られた場合、セキュリティ業務管理サーバ S_3 はユーザ U_1 に対して回答/指示を返す。このとき、後述する証拠情報の作成のために処理⑤で与えられたセッション鍵 SSK_2 を利用する。一方、セキュリティ業務管理サーバ S_3 は、事前に身分証明ID管理サーバ S_2 からユーザ U_1 に関する情報を受け取っている(処理⑥)ので、悪質なユーザ U_2 がユーザ U_1 であると偽ってメッセージの信託を依頼してきても、これを拒否することができる。なお、身分証明ID管理サーバ S_2 とセキュリティ業務管理サーバ S_3 の間では取扱に機密性を要する情報の交換が行われるので、この両者を繋ぐ通信路については十分に保護しておく。例えば、特殊な保護チャネルを使用する、 S_2 および S_3 に対するアクセス管理を厳格に行う、 S_2 および S_3 専用の暗号鍵で暗号化してデータ通信を行う、などによって通信路の保護を図る。

【0028】図7は、メッセージの信託に際して指定される信託条件 CU_2 の一例を示す図であり、ユーザ U_1 は自己のメッセージ M_1 を公開指定日時 T_1 が到来したときユーザ U_3 に対して公開する、という条件であるものとする。また、ユーザ U_1 はセキュリティ業務管理サーバ S_3 に信託するメッセージ M_1 の保護手段(どのような機密性、完全性、アクセス制御、否認不可及び監査機能を提供するか)についても信託条件 CU_2 で規定する。例えば図7において、機密性レベル=2、完全性レベル=1と指定されているので、メッセージ M_1 のデータ全体を暗号化するとともに改竄検出のためのコードを付加する。また、破棄指定日時 T_3 が指定されているので、時刻 T_3 を過ぎたときにメッセージ M_1 は破棄される。

【0029】図8は、図6のデータ通信における機密保護のための処理の流れを示すフローチャート(その1)である。同図中、ユーザ U_1 は自己の秘密鍵 SK_{U1} 、セキュリティ業務管理サーバ S_3 の公開鍵 PK_{S3} 、指定されていけばセッション鍵 SSK_2 を用いて、信託するメッセージ M_1 を暗号化する。原則的に、これらの暗号鍵を用いて暗号化してあれば、メッセージの内容を悪質なユーザ U_2 に盗み見られる可能性は少ないと期待されるが、“文書”としての効力をより確実なものとするには、メッセージ M_1 の作成者がユーザ U_1 であることを保証する証拠情報 E_1 と送信するメッセージ M_1 が原本であることを保証する証拠情報 E_2 とをメッセージ M_1 に付加する。この証拠情報 E_1 および E_2 の作成については、セキュリティ業務管理サーバ S_3 に作成させても、信頼できる第三者機関に作成処理を依頼してもよい(請求項中の“証拠情報作成手段”に相当する)。図8では、信託するメッセージ M_1 および作成日時情報 T_0 をユーザ U_1 の秘密鍵 SK_{U1} で暗号化したものを証拠情報 E_1 とする。さらに、原本性を保証する目的でセキュリティ業務管理サーバ S_3 から与えられたセッション鍵 SSK_3 を用いて、証拠情報 E_1 を付加したメッセージ M_1 を変換したものを証拠情報 E_2 とする。そして、メッセージ

M_1 に証拠情報 E_1 および E_2 を付加したものを自己の秘密鍵 SK_{U1} 、セキュリティ業務管理サーバ S_3 の公開鍵 PK_{S3} 、指定されていけばセッション鍵 SSK_2 を用いて暗号化することでメッセージ M_2 を作成し(ステップ801)、このメッセージ M_2 を実際にネットワーク N を介してセキュリティ業務管理サーバ S_3 に送信する(ステップ802)。セキュリティ業務管理サーバ S_3 は、ネットワーク N を介してメッセージ M_2 を受信すると、セッション鍵 SSK_2 、ユーザ U_1 の公開鍵 PK_{U1} 、自己の秘密鍵 SK_{S3} を用いてメッセージ M_2 から元の情報 I (メッセージ M_1 、証拠情報 E_1 および E_2)を復元して、これらの情報を信託条件 CU_2 にしたがって管理されるメッセージDB(図示なし)内に安全に保管する。メッセージDBに保管されたメッセージおよび証拠情報は図9のフローチャートにしたがって管理されており、信託条件 CU_2 の条件が満たされてメッセージ公開処理が行われないう限り、どんなユーザに対しても内容が公開されることはない。

【0030】図10は、図6のデータ通信で作成された証拠情報を確認する処理の流れを示すフローチャートである。以下、受信したメッセージ M_2 からセキュリティ業務管理サーバ S_3 が復元した元の情報の各々について、証拠情報を E_1' および E_2' 、メッセージを M_1' 、作成日時情報を T_0' としてユーザ U_1 から送信されたものと区別して表し、図10にしたがって説明を行う。

【0031】図10において、セキュリティ業務管理サーバ S_3 は、メッセージ M_2 から復元した証拠情報 E_1' をユーザ U_1 の公開鍵 PK_{U1} で復号化する(ステップ1001)。そして、得られた情報 I のうちのメッセージ M_1' とメッセージ M_2 から復元したメッセージ M_1' とを比較し、等しいか否かを調べる(ステップ1002)。このとき、必要があれば作成日時情報 T_0' についても確認する。メッセージ M_1' および M_1' が等しい場合、メッセージ M_1' がユーザ U_1 に作成されたものであることが確認されるので、次に、メッセージ M_2 から復元したメッセージ M_1' および証拠情報 E_1' に対してセッション鍵 SSK_3 を入力パラメタとしてハッシュ関数を施し、証拠情報 E_2' を作成する(ステップ1003)。なお、ユーザ U_1 およびセキュリティ業務管理サーバ S_3 は、同一のハッシュ関数を極秘に共有しているものとする。この後、メッセージ M_2 から復元した証拠情報 E_2' と証拠情報 E_2' とが等しいか否かを調べる(ステップ1004)。証拠情報 E_2' および E_2' が等しい場合、メッセージ M_1' は原本であって途中で改竄されていないことが確認される。以上のようにしてネットワーク N を介して受信したメッセージ M_2 から復元した情報 I の正当性が確認された後(図8中のステップ804)、セキュリティ業務管理サーバ S_3 はメッセージ M_1' と証拠情報 E_1' および E_2' をメッセージDBに保管する。

【0032】ユーザ U_1 が指定した信託条件 CU_2 の条件が満たされる(公開指定日時 T_1 が到来する)と、セキュリ

ティ業務管理サーバS₃は、信託条件C_{U₂}に基づき、公開対象のユーザU₃にメッセージM₁' (=M₁)を公開する。このとき、セキュリティ業務管理サーバS₃は、メッセージDB中に保管しておいたメッセージM₂の取り出し、その内容確認、メッセージM₁'の作成者がユーザU₁であることおよび原本であることの確認などを、図10に示したのと同様の手順で行う。

【0033】図11は、図6のデータ通信における機密保護のための処理の流れを示すフローチャート(その2)であり、図10の確認処理に引き続いてセキュリティ業務管理サーバS₃がメッセージM₁を公開対象のユーザU₃に送信する処理(図6中の処理⑨に相当する)を示す。このデータ通信に際しても、セキュリティ業務管理サーバS₃の秘密鍵SK_{S₃}およびユーザU₃の公開鍵PK_{U₃}によってメッセージM₁を暗号化して送信する。ユーザU₃本人であれば、受信した暗号化メッセージを自己の秘密鍵SK_{U₃}で解読可能であり、セキュリティ業務管理サーバS₃の公開鍵PK_{S₃}で解読することによって受信した暗号化メッセージが間違いなくS₃に保証されたものであることを確認できる。また、図11においてM₃はセキュリティ業務管理サーバS₃が添付して送信するメッセージである。

【0034】次に、メッセージM₁を信託したユーザU₁とメッセージM₁を公開されたユーザU₃との間で信託メッセージの送受信に関する紛争が発生したときにセキュリティ業務管理サーバS₃が果たすべき役割について述べる。メッセージM₁を信託する側のユーザU₁とセキュリティ業務管理サーバS₃の間では、前述した証拠情報E₁およびE₂を作成することによって処理過程にかなりの機密度が保証される。しかしながら、メッセージM₁を受け取る側のユーザU₃については、以下に示すような原因からトラブルが発生する可能性がある。

(A) ユーザU₃がメッセージM₁を受け取った旨の応答を行わない。

(B) ユーザU₃がM₁と異なるメッセージを受け取ったと主張する。

(C) ユーザU₃の管理不全により、悪質なユーザU₂にメッセージM₁を盗用される。

【0035】上記(A)のケースについては、信託条件C_{U₂}の中で信託メッセージの受け渡し方を規定しておくことにより、トラブルの解決および発生防止を図ることができる。例えば、信託メッセージの送信リトライ回数を指定したり、義務付けた応答をユーザU₃が返してこない場合には受信したものと解釈する、などである。この他、信頼できる配送サーバを通信経路の途中に設けて、データ通信が行われたことを示すE₃を作成しておくことなども有効である。

【0036】上記(B)のケースについては、前述した証拠情報E₁、E₂、E₃をユーザU₃に提示することで、トラブルの解決および発生防止を図ることができる。すなわ

ち、証拠情報E₁によってメッセージM₁が間違いなくユーザU₁に作成されたことを、証拠情報E₂によってメッセージM₁の原本性(修正されずに保管されていたこと)を、証拠情報E₃によって信託されたときの状態でセキュリティ業務管理サーバS₃からユーザU₃にメッセージM₁が渡されたことを、それぞれ証明できる。

【0037】上記(C)のケースについては、ユーザU₃の責任によることが明らかであるが、セキュリティ業務管理サーバS₃は、ユーザU₃に対してメッセージM₁を送信する以前にメッセージM₁の内容が漏洩したのではないことをセキュリティ監査機能によって証明して、トラブルの解決および発生防止を図ることができる。図12は、セキュリティ監査機能を概略的に示すフローチャートであり、セキュリティ関連の事象についてのメッセージの収集手段、メッセージ分析手段、メッセージ記録手段、メッセージ選択手段、セキュリティレポート作成手段などを有する(請求項中の「履歴情報取得手段」に相当する)。そして、得られたセキュリティレポートの情報を分析し、ネットワークシステム全体の弱点を診断する手段(請求項中の「セキュリティ侵害監査手段」に相当する)も提供されているので、これを利用して上記の証明を行うことは可能である。なお、セキュリティ監査機能の詳細については、本出願人による特願平6-47194号出願に添付した明細書「セキュリティ管理装置」に記載があるので、説明を省略する。

【0038】

【発明の効果】以上詳しく説明したように、本発明のメッセージの信託システムによれば、身分証明ID登録手段は身分証明IDによって特別なセキュリティ業務を利用するユーザの身元を保証し、セキュリティ業務管理手段は身分証明IDによる身元の保証が完了しているユーザに対してのみメッセージの信託サービスなどのセキュリティ業務を提供するので、不正に情報を取得しようとする意図を持つ悪質なユーザを容易に選別および排除することができるという効果が得られる。そして、信託メッセージ秘匿手段はネットワーク経由で送受信されるメッセージの内容を暗号化して、当該メッセージに関わるユーザおよびセキュリティ業務管理手段以外の第三者に知られないようにするので、仮に悪質なユーザにメッセージを取得された場合でも、その盗用などによる損失の発生を未然に防止することができるという効果が得られる。

【0039】また、証拠情報作成手段は身分証明IDによってセキュリティ業務を利用するユーザのWSから送信されてきたメッセージについて生成および送受信が行われた事実を証明するための証拠情報を作成するので、セキュリティ業務を利用するユーザの間で紛争が発生した場合、保管しておいた証拠情報を調べることによって紛争の原因を客観的に突き止めることができるという効果が得られる。そして、改竄防止手段はメッセージの当

事者（例えば、メッセージを作成および送信したユーザと、当該ユーザに対してセキュリティ業務を提供するセキュリティ業務管理手段）以外の第三者に改竄されないようにメッセージのデータ形式を変換するので、メッセージの内容についての信頼性を向上させることができるという効果が得られる。

【0040】さらに、履歴情報取得手段は稼働中のシステム内で発生した事象を履歴情報として絶えず記録しており、セキュリティ侵害監査手段は記録された履歴情報を常に分析しているので、悪質なユーザによるセキュリティ侵害を迅速に検出して、早期に適切な処置をとることができるという効果が得られる。

【図面の簡単な説明】

【図1】本発明のメッセージの信託システムの一構成例を示すブロック図である。

【図2】身分証明IDの発行要求に伴って図1のシステムで行われるデータ通信について概略的に示す図である。

【図3】図2のデータ通信における機密保護のための処理の流れを示すフローチャートである。

【図4】身分証明IDの登録および発行処理に伴って図1のシステムで行われるデータ通信について概略的に示す図である。

【図5】図4のデータ通信における機密保護のための処理の流れを示すフローチャートである。

【図6】メッセージの信託処理に伴って図1のシステムで行われるデータ通信について概略的に示す図である。

【図7】メッセージの信託に際して指定される信託条件の一例を示す図である。

【図8】図6のデータ通信における機密保護のための処理の流れを示すフローチャート（その1）である。

【図9】図6のデータ通信で信託されたメッセージを保管する処理の流れを概略的に示すフローチャートである。

【図10】図6のデータ通信で作成された証拠情報を確認する処理の流れを示すフローチャートである。

【図11】図6のデータ通信における機密保護のための処理の流れを示すフローチャート（その2）である。

10 【図12】図1中のセキュリティ監査機能を概略的に示すフローチャートである。

【符号の説明】

N ネットワークシステム

S₁ 身分証明ID発行サーバ

S₂ 身分証明ID管理サーバ

S₃ セキュリティ業務管理サーバ

WS₁₀, WS₂₀, WS₃₀ ワークステーション

U₁, U₂, U₃ ユーザ

PU₁ ユーザU₁の身分証明ID

20 PU₁' PU₁の引替え証

PK_{U1}, PK_{U3}, PK_{S1}, PK_{S2}, PK_{S3} 公開鍵

SK_{U1}, SK_{U3}, SK_{S1}, SK_{S2}, SK_{S3} 秘密鍵

SSK₁, SSK₂, SSK₃ セッション鍵

M, M₁, M₂, M₃, M₁' メッセージ

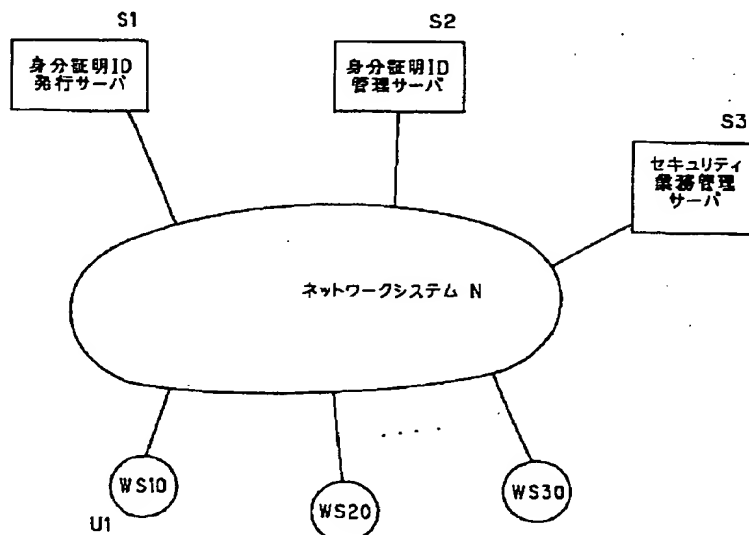
T₀, T₁, T₃, T₄, T₀' 時刻情報

E₁, E₂, E₃, E₁', E₂' 証拠情報

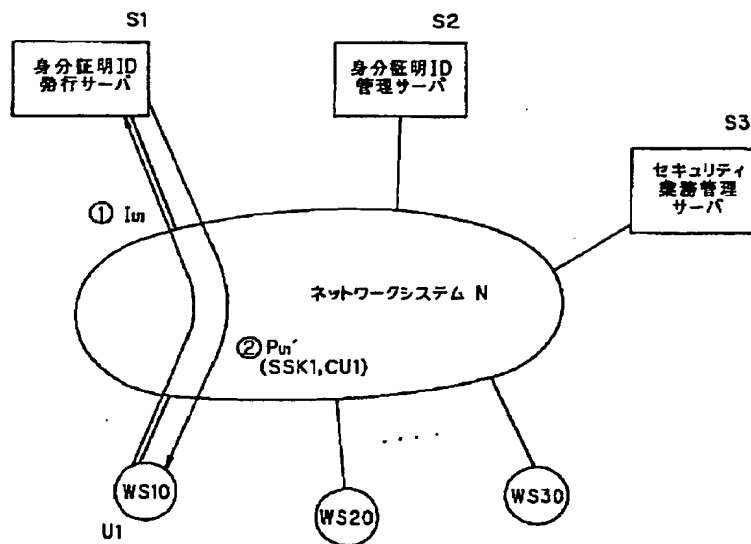
ENC 暗号化関数

DEC 復号化関数

【図1】

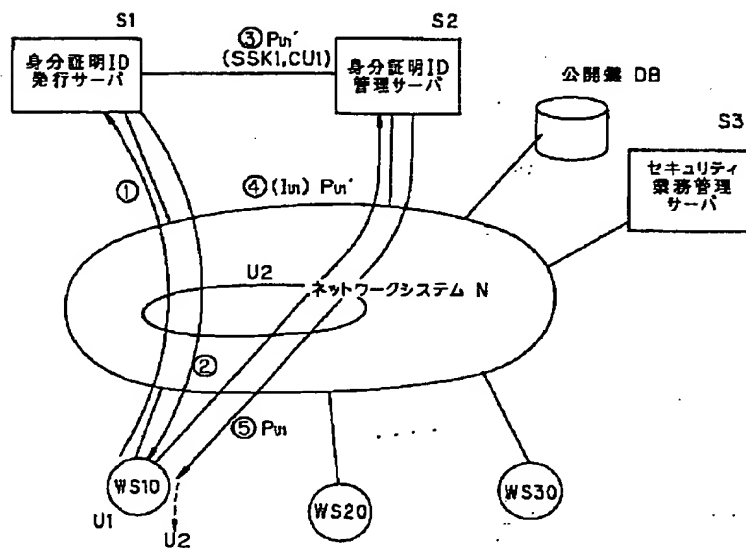


【図 2】



【図 2】

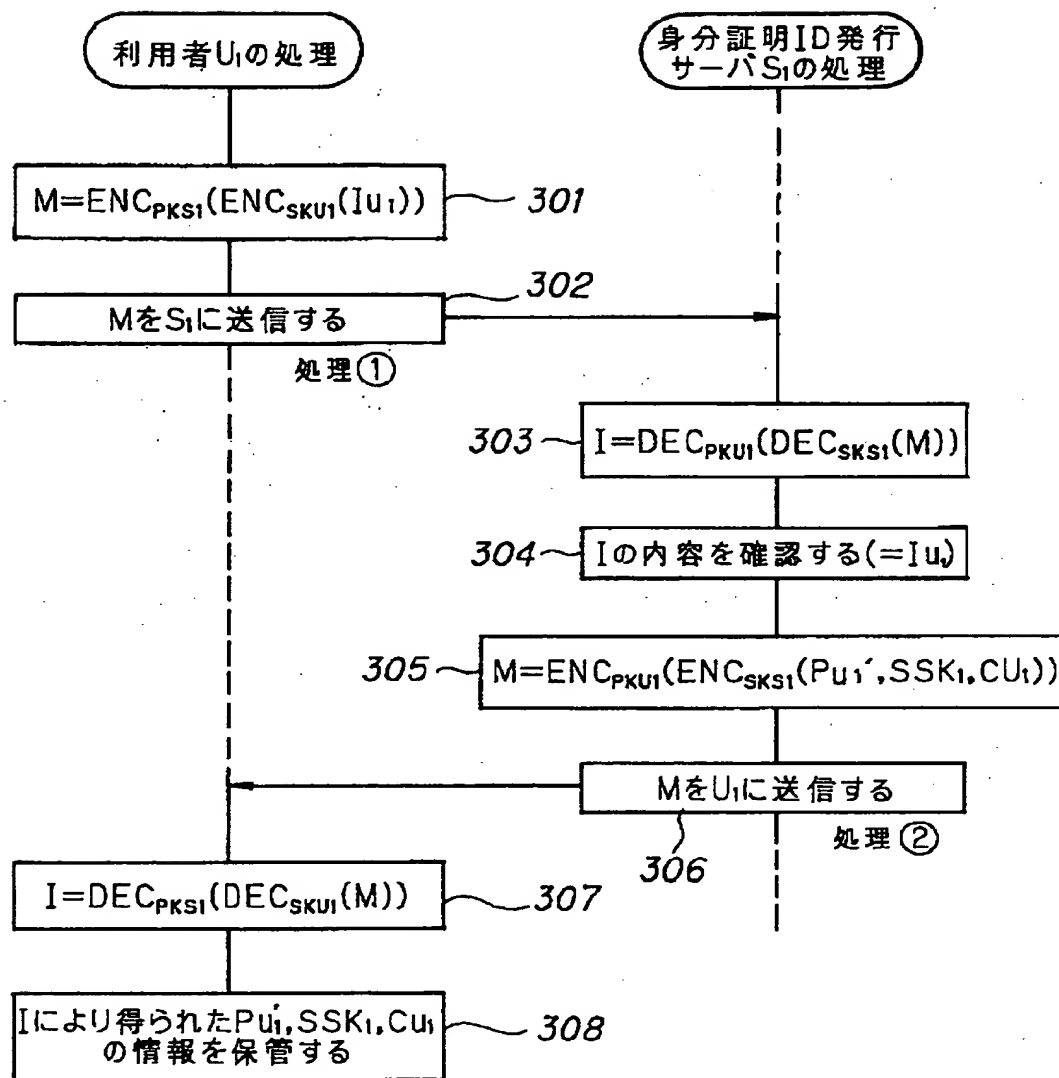
【図 4】



【図 4】

【図3】

【図3】



(凡例)

ENC: 暗号化関数

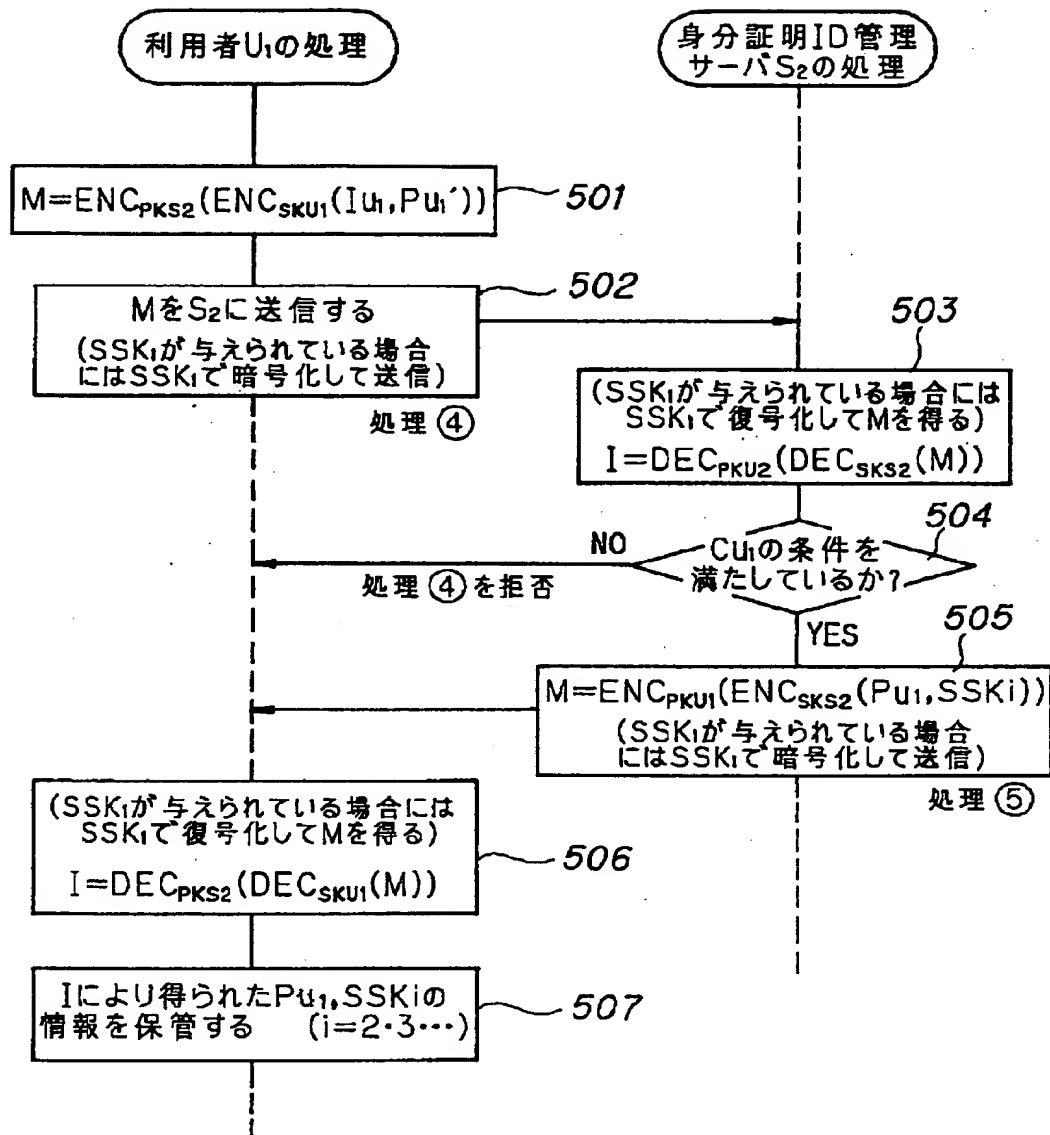
DEC: 復号化関数

M: 暗号化により作成したメッセージ

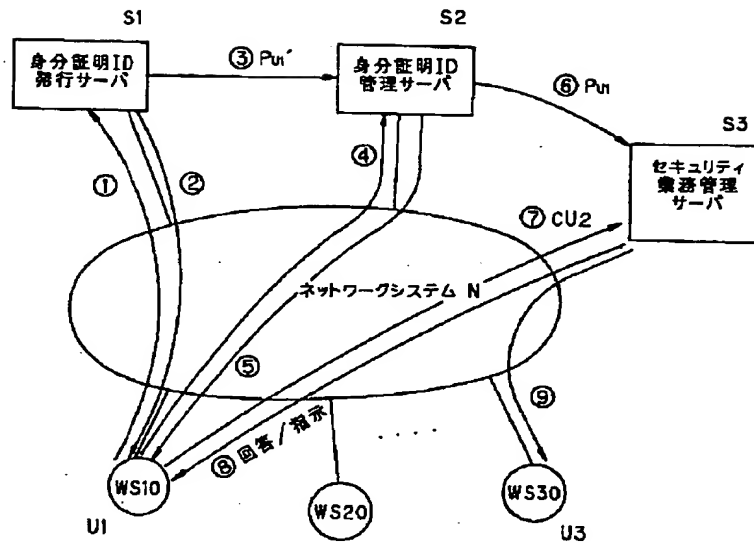
I: 復号化により得た情報

【図5】

【図5】



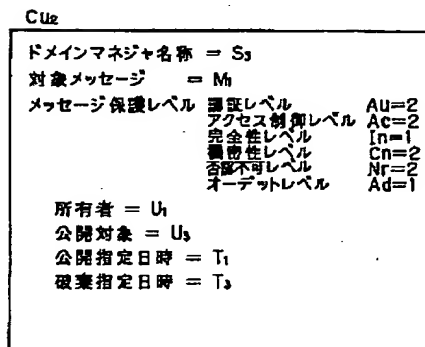
【図6】



【図6】

【図7】

【図7】

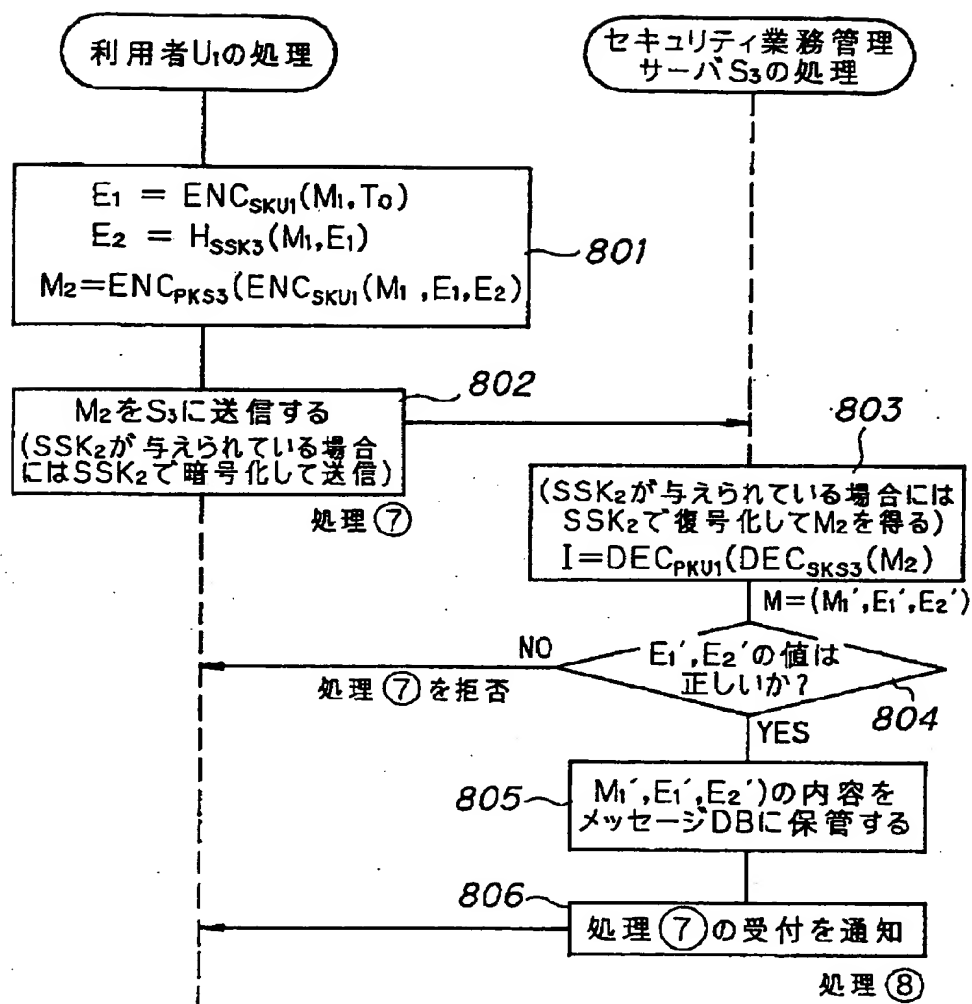


(凡例)

- | | |
|--|---|
| <p>認証レベル AU</p> <p>0: 認証を行わない</p> <p>1: ログイン時のみの認証</p> <p>2: 定期的にパスワード入力による認証</p> | <p>否認不可レベル</p> <p>0: 否認不可を行わない</p> <p>1: 送信時の証明作成</p> <p>2: 配送時の証明作成</p> |
| <p>アクセス制御レベル Ac</p> <p>0: アクセス制御を行わない</p> <p>1: 自システム内のみアクセス制御</p> <p>2: 他システムも含んだアクセス制御</p> | <p>オードットレベル</p> <p>0: オードットを行わない</p> <p>1: アラーム情報の取得</p> <p>2: セキュリティ報告書の作成</p> |
| <p>完全性レベル In</p> <p>0: 完全性の保護をしない</p> <p>1: 検出コード付加</p> <p>2: デジタル署名</p> | |
| <p>機密性レベル Cn</p> <p>0: 機密性の保護をしない</p> <p>1: データの一部の保護</p> <p>2: データ全体の保護</p> | |

【図8】

【図8】



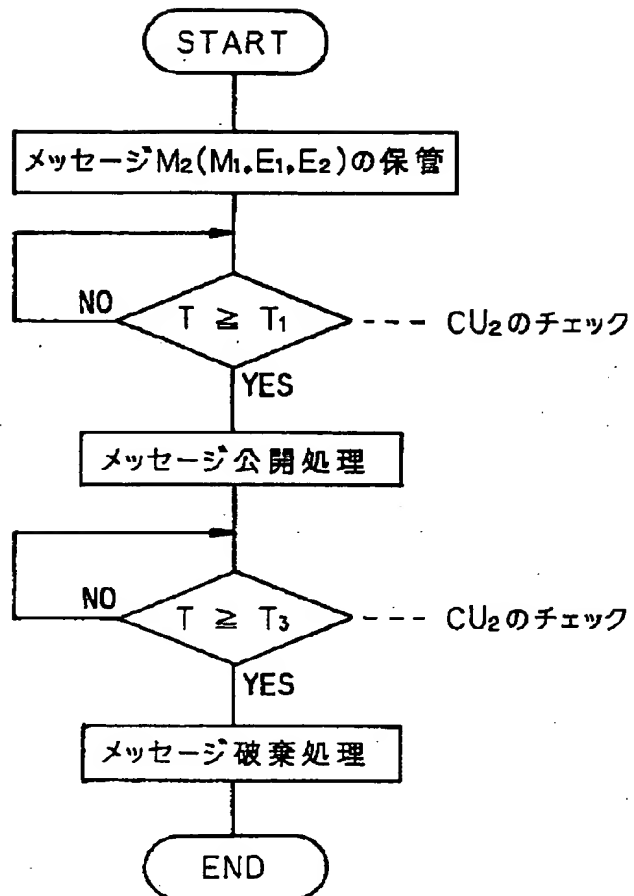
(凡例)

H : 証拠情報作成用のハッシュ関数

E₁, E₂ : 利用者U₁が作成した証拠情報E₁', E₂' : サーバS₃が受信した証拠情報M₁' : サーバS₃が受信したメッセージ

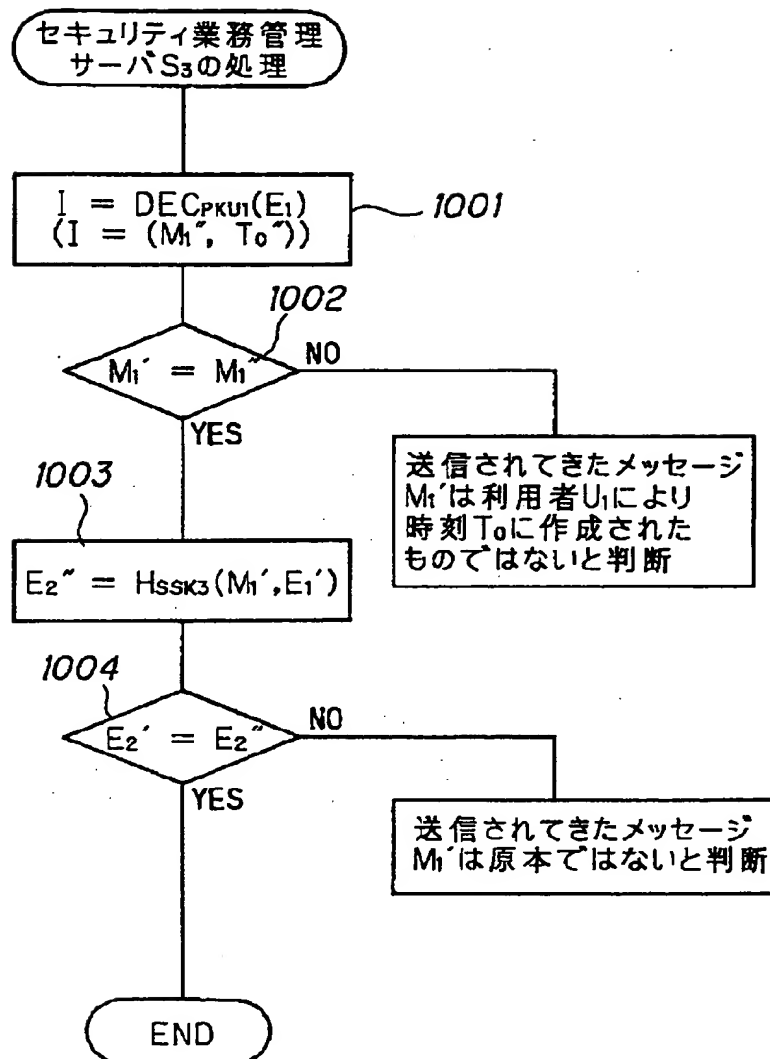
【図9】

【図9】



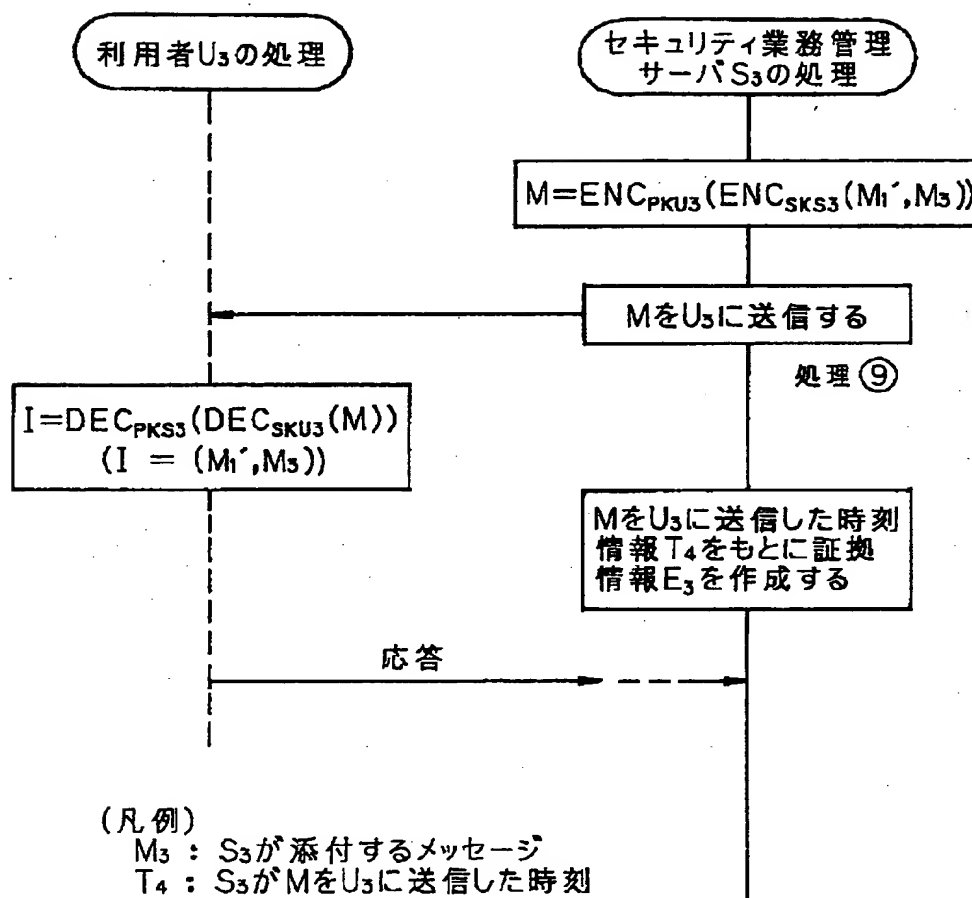
【図10】

【図10】



【図11】

【図11】



【図12】

【図12】

